IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 3-7 and 9-15, and CANCEL claims 16-26, without prejudice or disclaimer, in accordance with the following:

1. (PREVIOUSLY PRESENTED) A cryptographic method comprising:

receiving physical characteristic information representing a characteristic inherent to an individual;

randomly determining a numeric key;

generating a cryptographic key from said numeric key and a predetermined primary key;

encrypting said physical characteristic information using said cryptographic key; and

generating an auxiliary code for decrypting said cryptographic key, from said encrypted physical characteristic information and said numeric key.

2. (PREVIOUSLY PRESENTED) A decryption method comprising:

receiving encrypted physical characteristic information and an auxiliary code;

restoring a numeric key from said received encrypted physical characteristic information and said auxiliary code;

restoring cryptographic key from said numeric key and a predetermined primary key; and

decrypting said encrypted physical characteristic information by using said cryptographic key and obtaining physical characteristic information.

3. (CURRENTLY AMENDED) A cryptographic equipment, comprising:

an inputting ~~means for~~unit inputting physical characteristic information representing a characteristic inherent to an individual;

a numeric key generating ~~means for~~unit randomly determining numeric key;

a key generating ~~means for~~unit generating a cryptographic key from said numeric key and a predetermined primary key;

an encrypting ~~means for~~unit encrypting said physical characteristic information using said cryptographic key; and

a code generating ~~means for~~ unit generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

4. (CURRENTLY AMENDED) A decryption equipment comprising:

a receiving ~~means for~~unit receiving an encrypted physical characteristic information and an auxiliary code;

a numeric key restoring ~~means for~~unit restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;

a key generating ~~means for~~unit generating a cryptographic key from said numeric key and a predetermined primary key; and

a decrypting ~~means for~~unit decrypting said encrypted physical characteristic information by using said cryptographic key.

5. (CURRENTLY AMENDED) A storage media ~~for~~ storing a program to read and be executed by a computer, comprising:

~~a~~ an inputting procedure ~~for~~ inputting physical characteristic information representing a characteristic inherent to an individual;

a numeric key generating procedure ~~for~~ randomly determining a numeric key;

a key generating procedure ~~for~~ generating a cryptographic key from said numeric key and a predetermined primary key;

an encrypting procedure ~~for~~ encrypting said physical characteristic information using said cryptographic key; and

a code generating procedure ~~for~~ generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

6. (CURRENTLY AMENDED) A storage media ~~for~~ storing a program to read and be executed by a computer, comprising:

a receiving procedure ~~for~~ receiving a cryptogram including an encrypted physical characteristic information and an auxiliary code;

a numeric key restoring procedure ~~for~~ restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;

a key generating procedure ~~for~~ generating a cryptographic key from said numeric key and a predetermined primary key; and

a decrypting procedure ~~for~~ decrypting said encrypted physical characteristic information

by using said cryptographic key.

7. (CURRENTLY AMENDED) A cryptographic method comprising:

receiving physical characteristic information representing a characteristic inherent to an individual;

arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

encrypting the scrambled physical characteristic information by using ~~the~~ a predetermined cryptographic key.

8. (PREVIOUSLY PRESENTED) A decryption method comprising:

receiving a cryptogram which is an encryption of scrambled physical characteristic information;

decrypting said cryptogram by using the predetermined cryptographic key and obtaining said scrambled physical characteristic information; and

descrambling said scrambled physical characteristic information by removing each element from each component constructing the result of decryption, in which each element is effected at the time of scrambling, by a plurality of components that has a predetermined relationship with said each component.

9. (CURRENTLY AMENDED) A cryptographic equipment comprising:

an inputting ~~means for~~unit inputting physical characteristic information representing a characteristic inherent to an individual;

a scrambling ~~means for~~unit arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

an encrypting ~~means for~~unit encrypting the scrambled physical characteristic information by using the predetermined cryptographic key.

10. (CURRENTLY AMENDED) A decryption equipment comprising:

a decrypting ~~means for~~ unit decrypting a received cryptogram which is an encryption of a

scrambled physical characteristic information, by a predetermined cryptographic key and obtaining said scrambled physical characteristic information; and

a descrambling ~~means for~~unit descrambling said scrambled physical characteristic information.

11. (CURRENTLY AMENDED) A storage media ~~for~~ storing a program to read and be executed by a computer, comprising:

~~a~~ an inputting procedure ~~for~~ inputting physical characteristic information representing a characteristic inherent to an individual;

a scrambling procedure ~~for~~ arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information; and

an encrypting procedure ~~for~~ encrypting the scrambled physical characteristic information by using the predetermined cryptographic key.

12. (CURRENTLY AMENDED) A storage media ~~for~~ storing a program to read and be executed by a computer, comprising:

a decrypting procedure ~~for~~ decrypting a received cryptogram which is an encryption of a scrambled physical characteristic information, by a predetermined cryptographic key and obtaining said scrambled physical characteristic information; and

a descrambling procedure ~~for~~ descrambling said scrambled physical characteristic information.

13. (CURRENTLY AMENDED) A remote identification system, comprising:

a client-side equipment comprising

an inputting ~~means for~~unit inputting physical characteristic information representing a characteristic inherent to an individual,

a proof information inputting ~~means for~~unit inputting information including identifier or identifying the individual and a password,

an encrypting ~~means for~~unit encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram, and

an outputting ~~means for~~unit outputting authenticating information generated from said cryptogram and said identifier; and

a server-side equipment comprising

a registering ~~means for~~unit registering said password and reference data, which is obtained by measuring a physical characteristic corresponding to each individual, relating to a given identifier corresponding to each individual,

a receiving ~~means for~~unit receiving authenticating information comprising said cryptogram and said identifier,

a retrieving ~~means for~~unit retrieving a relating password and reference data from said registering ~~means~~ unit in accordance to said received identifier,

a decrypting ~~means for~~unit decrypting said received cryptogram by using the password retrieved by said retrieving ~~means~~ unit as a cryptographic key and obtaining a physical characteristic information, and

an examining ~~means for~~unit examining whether or not said physical characteristic information and said retrieved reference data are equivalent.

14. (CURRENTLY AMENDED) A data sending equipment, comprising:

an inputting ~~means for~~unit inputting physical characteristic information representing a characteristic inherent to each individual;

a proof information inputting ~~means for~~unit inputting information including identifier or identifying an individual and a password;

an encrypting ~~means for~~unit encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram; and

an outputting ~~means for~~unit outputting authenticating information generated from said cryptogram and said identifier.

15. (CURRENTLY AMENDED) An identifying equipment, comprising:

a registering ~~means for~~unit registering password and reference data, which is obtained by measuring a physical characteristic corresponding to each individual, relating to given identifier corresponding to each person;

a receiving ~~means for~~unit receiving authenticating information comprising said cryptogram and said identifier;

a retrieving ~~means for~~unit retrieving a relating password and reference data from said registering ~~means~~ unit in accordance to said received identifier;

a decrypting ~~means for~~unit decrypting said received cryptogram by using the password retrieved by said retrieving ~~means~~ unit as a cryptographic key and obtaining a physical

characteristic information; and

an examining ~~means for~~unit examining whether or not said physical characteristic information and retrieved reference data are equivalent.

16-26 CANCELLED